Design Document[1]

Web-based Submission of the Discharge Monitoring Report[2]

EPA Contract #68-W5-0030[3]

Delivery Order #0004

Revised August 30, 1999

[1] Deliverables 2.2 & 2.3, Information Dynamics, Inc.

[2] A field test in the State of New York of the digital signing and submission of the Discharge Monitoring Report using an Adobe Acrobat Exchange plug-in to a Web browser as the electronic form environment which is connected interactively across the Internet to a receiving Web site. Cryptographic and handwritten biometric digital signatures are evaluated in this pilot.

[3] Submission of Environmental Data Under the Taiwan-USEPA Technical Cooperation Agreement

1 Scope

This Design Document describes the high-level design of a pilot test of the Web-based submission of the New York State Discharge Monitoring Report (DMR) conducted in the State of New York June – November, 1999. This document describes what questions are addressed by this pilot, how these questions motivate specific tests, and how these tests will be accomplished.

In the pilot test, seven facilities which submit the New York version of the Discharge Monitoring Report to the New York State Department of Environmental Conservation (NYS-DEC) will fill out an electronic version of the DMR which each pilot participant can select from a Web site which has been established for the pilot. After the pilot participant has completed the electronic DMR, the pilot participant will sign the DMR with a digital signature and then submit the signature and DMR data to a receiving Web site, which will accept the data and verify the signature. The receiving Web site will make the submitted data available to the New York State Department of Environmental Conservation (NYS DEC).

2 Questions To Be Addressed by Pilot

Since, compared with other environmental compliance reports, the Discharge Monitoring Report (DMR) is more frequently involved in litigation, and since this litigation, when it occurs, often seeks to prove criminal fraud by showing that the DMR was filed with false information by a specific individual, electronic DMRs raise the legal question:

> How can an individual be held responsible for the content of an electronic DMR?

For the purposes of the pilot, this question, which has its origin in a legal requirement, motivates a technical design for the DMR pilot which attempts to ensure that:

- A consistent correspondence exists between the electronic representation of the DMR which is digitally signed and the full context of what the submitter of the DMR sees displayed on the screen of the submitter’s computer, such that the signing of the electronic representation of the DMR could be argued as equivalent to the signing of the visual representation of the DMR as experienced by the submitter when the digital signature is applied.

- The DMR form is under the control of the submitter at the moment of signing, in the sense that the entire electronic representation of the DMR form (template plus data) exists in the memory of the submitter's computer at the time the digital signature is applied.
- The entire contents (template plus data) of the DMR form is digitally signed, and this signature occurs on the submitter's computer at the time the submitter is viewing the DMR form and executing the signature.
- Submitted DMR data are received within a short period of time after the electronic representation of the DMR has been signed by the submitter, so that a meaningful time stamp can be applied to the submitted data at the receiving site.
- The transmission of submitted data to the receiving site from the submitter's computer can be shown to be within the same network session in which the submitter selected a specific DMR version (containing a specific permit number) to complete and sign, so that a direct and constrained chain of custody for the submitted DMR data can be shown.
- Once submitted DMR data are received at the receiving site, the receiving site can verify that the submitted data: 1) were signed by a specific individual, 2) were signed in the context of the complete DMR form, and 3) were not altered since signing.

- The submitter can subsequently inspect all of the data received by the receiving site in the context in which it was originally signed and submitted.

Because the DMR is one of the more frequently litigated compliance reports, the pilot test was designed to establish an “upper limit” to the technical methods employed to ensure that a submitted electronic DMR could be shown to have been signed by a specific individual. A risk judgment could then be made for other compliance reports to determine to what degree these methods could be relaxed to satisfy potentially lesser requirements for authentication of digital signatures.

In addition to the security and authentication question discussed above, and being aware that measures to increase security and authentication can decrease ease of use, the DMR pilot also seeks to answer the question:

> In what ways are the signing and submission of an electronic DMR found to be easy or difficult by the pilot participants?

This question relates to the subjective, “human factors” experience of the pilot participants with the pilot test configuration from initial setup through final submission. Both the “security” and “human factors” questions are explored in more detail in the subsections below.

7.1 Questions Related to Digital Signatures

The broad question as stated above, “How can an individual be held responsible for the content of an electronic DMR?” is related to the way in which a digital signature is applied and interpreted. The DMR pilot will test both a cryptographic and biometric digital signature mechanism. Questions related to digital signatures which motivate the design of the DMR pilot include:

- Can a workable public key infrastructure be established which links the signer’s private cryptographic key to the signer’s identity by means of a security policy which can be used by the New York State Department of Environmental Conservation and the pilot participants and which also binds the private key to the signer’s identity with a sufficient level of assurance?
- Can private keys be implemented on a hardware token (smart card) in a manner which is usable by the pilot participants and is compatible with a mechanism for applying cryptographic signatures to the DMR?
- Is it feasible to sign the DMR form with a biometric handwritten signature? How accurate is the verification of the handwritten signature based on an enrollment of sample signatures by the pilot participants?

10.1 Questions Related to Human Factors

In the DMR pilot, many procedures and hardware/software components will be introduced, many of which are designed to minimize the risk that the signer's identity cannot be linked to DMR at a sufficient level of assurance required to satisfy the need for legal enforceability. The DMR pilot will test the degree to which the pilot participants can understand these procedures and use these components, and will seek to collect data on the ease-of-use (human factors) involved in the electronic form environment for the DMR, the enveloping context of Web menus and selections provided by the receiving Web site, and the procedures and tools needed to execute both cryptographic and biometric signatures. Specific questions related to human factors include:

- How long and how difficult will the pilot participants find the process of installing the hardware and software components needed for the pilot? What average times and kinds of difficulty are experienced in each installation step?
- Will the pilot participants understand the meaning and purpose of digital signatures? Will the concept of digital signatures be accepted as intuitively obvious? What types of errors related to the submitter's understanding of the digital signature will emerge? What types of technical errors will emerge?
- How will the pilot participants experience the setup processes required to participate in a public key infrastructure for the purpose of using a cryptographic digital signature?
- How intuitive (or difficult) will pilot participants find the use of special pen and graphics tablet to apply a biometric signature which mimics a traditional handwritten signature?
- How will a prompt which asks the submitter to indicate the meaning of the digital signature be received by the pilot participants, and what difference will such a prompt make in their understanding or experience of the signing process?
- How intuitive will the pilot participants find the electronic forms environment used to display the contents of the DMR form and accept data entry from the submitter?
- How intuitive will the pilot participants find the process of using the receiving Web site, including the process of logging into the receiving Web site, finding and selecting the appropriate DMR?

17.1 Questions Related to Implementation Options

The DMR pilot will be implemented with an electronic form plug-in to a Web browser on the submitter's computer which will access a receiving Web site across the Internet. Hardware-based cryptographic and biometric signatures will be tested, both of which require the installation of hardware devices to the submitter's computer. A complete public key infrastructure (PKI) will be implemented for the pilot in which the pilot participants enroll at the certificate authority's Web site to generate certificate requests which are then approved via a Web-based administrative console by the New York State Department of Environmental Conservation acting as the Local Registration Authority within the PKI.

The receiving Web site will serve DMR forms in the electronic form environment which are prepopulated with data dependent on the submitter's login ID and also upon the submitter's specific selections of monitoring period, discharge number (or comment), and version of the form. The receiving Web site will store data entered by the submitter in a database and will verify the digital signatures which have been applied to the DMR form by the submitter. The receiving Web site will also send submitted data files containing a copy of both the submitted and pre-populated DMR data to the New York State Department of Environmental Conservation using E-mail attachments as the transport mechanism. The ability to view all of the submitted DMR forms using a Web browser and the electronic form environment will be granted to the New York State Department of Environmental Conservation. The ability to view all the DMR forms which have been submitted by a given facility will be granted to all login IDs which are associated with the facility.

Given the above specific implementation for the DMR pilot, questions related to this implementation include:

- What compatibility restrictions will be discovered among the different software products used to produce the integrated functionality for the pilot?
- What specific problems or behaviors will be observed when the pilot participants install hardware devices on their computers?
- Will the configuration of software and hardware components installed for the DMR pilot behave similarly across all of the pilot participants' computers, or will differences in some or all pilot participants' computers result in a divergent set of behaviors observed for the installed hardware/software configuration?
- Will the pilot participants experience difficulty in connecting to the receiving Web site established for the DMR pilot across their respective network connections, including dial-up lines?
- Will the pilot participants or the Local Registration Authority administrator experience difficulty in connecting to the certificate authority server across their respective network connections?

- Can the pilot participants switch between standard Web pages and the electronic form environment with acceptable responsiveness?
- Will the process of pre-populating the DMR forms with data from the receiving site's database occur with reasonable responsiveness?
- Can the digital signature applied to the DMR form by the submitter be verified at the receiving site with sufficient speed to notify the submitter of the success or failure to verify shortly after the DMR form is submitted to the receiving site?
- Can the New York State Department of Environmental Conservation successfully receive the submitted data files shortly after the submitted DMR data have been received?
- Is the version control applied to the submitted components of the DMR (e.g., discharge numbers and comments) sufficient for the New York State Department of Environmental Conservation to determine which components should be assembled to form a completed DMR and also to distinguish the most recent submission of any component from previous submitted versions?
- What scalability, maintainability, compatibility or security issues are raised by the specific implementation used for the DMR pilot?
- What alternative implementation options are suggested by the pilot experience?

30 How Pilot Tests will be Conducted

The DMR pilot will test the ability of the pilot participants to:

- install the software and hardware components used in the pilot,
- perform the necessary setup steps to prepare to use the digital signature mechanism,
- select the appropriate DMR using a Web interface,
- add data to the DMR form using an electronic form environment,
- execute the digital signature,
- submit the DMR form to the receiving Web site.

Features of the DMR pilot design which support these activities are discussed in detail in the subsections below, followed by a list of the test procedures.

36.1 Selection of Pilot Participants

Participants for the DMR pilot were selected by the New York State Department of Environmental Conservation among facilities which had previously filed New York State DMRs and currently held valid permits to discharge effluent into an open body of water. The New York State Department of Environmental Conservation invited facilities to participate in the pilot based on the following criteria:

- The facility files DMRs of three pages or less.
- The facility is located within a half-day's drive from Albany, New York[4].
- The facility is not currently out of compliance with their discharge permits.

The pilot participants, in turn, responded to the invitation based on their interest in participating in the pilot, and therefore self-selected themselves. The participants were required to provide a computer with a connection to the Internet (either network or dial-up) which they would make available to install the pilot's hardware and software components. The pilot participants were not reimbursed for their time working with the DMR pilot, other than the support the participating companies and organizations provided to their respective staff. The pilot participants attended an orientation meeting at the New York State Department of Environmental Conservation in Albany, New York, in January, 1999.

The DMR pilot participants represented the following companies and organizations:

- General Electric
- IBM
- Allied Signal
- Indeck Energy Systems of Ilion
- The Village of Champlain, New York
- Montgomery County Sanitation District Number 1
- Rosendale Waste Water Treatment Facility

46.1 Organization of the DMR Data Sets

The DMR pilot will establish a convention for organizing DMR data in data sets which can be selected by the submitter using a Web interface, and then pre-

[4] An invitation was also extended to IBM's centralized environmental reporting group in Manassas, VA, which prepares the New York State DMR report for IBM's Loral facility, which is located in New York State.

populated and presented to the submitter via an electronic form plug-in to the submitter's Web browser. For the purposes of the pilot, the New York State Discharge Monitoring Report (DMR) will be treated as a single compliance report related to a permit number and an end date for a particular monitoring period. Each DMR report is composed of one or more components. These components can be a report of measurements of parameters associated with a particular discharge number, or a comment which applies to the DMR submission as a whole.

Within the pilot, a DMR submission related to a particular permit number and end date for a monitoring period will be treated logically as an information container which can include multiple versions (separate submissions) of various discharge numbers and comments. Data will be collected, stored and transmitted to the New York State Department of Environmental Conservation packaged at the component (e.g., discharge number or comment) level.

The following diagram illustrates the relationship of the component data sets to the complete DMR submission.

The DMR permit holder ("permitee") can prepare multiple versions of each component of the complete DMR. When these versions are for the permitee's internal use, the versions are termed "internal versions" and are assigned an internal version number which increments as new versions of a given component (discharge number or comment) are prepared within the logical container described by a given permit number and end date. When a given component is signed and submitted to the New York State Department of Environmental Conservation, each instance of a given component's submission is termed an "external version" of the submitted component. Each submitted component (discharge number or comment) is assigned an external version number which increments as new versions of a given component are submitted. Internal and external version numbers are two separate and independent numbering schemes for a given component within a given information container described by the permit number and end date of the monitoring period.

Within the DMR pilot, the New York State Department of Environmental Conservation can potentially receive a boundless number of component submissions. A DMR is considered complete (for a given permit number and monitoring period end date) when all of its required components (discharge numbers) have been submitted. The comment component is optional. Although the receipt by the New York State Department of Environmental Conservation of a new version of a given component logically updates the DMR as a whole (for any given permit number and end date), version numbers are assigned only to each component of the DMR. Within the pilot there is no concept of separate versions for the DMR submission as a whole.

Data sets containing information particular to a given facility (e.g., facility name and location), and permit (e.g., parameters to be monitored, such as pH, temperature, quantity of a given chemical, etc., and limits for these parameters established by the permit) will be supplied to the receiving Web site by the New York State Department of Environmental Conservation for the purpose of pre-populating each DMR component with default information appropriate to a given permit and monitoring period. These data sets will be supplied to the receiving Web site from the New York State Department of Environmental Conservation as structured text files sent within E-mail attachments. The receiving Web site will store these data in a database maintained by the receiving Web site. Data submitted by the pilot participants will be collected by the receiving Web site, stored in a database and then extracted as a set of structured text files (which contain the full context of both the prepopulated and submitted data) and then sent to the New York State Department of Environmental Conservation according to a preset transmission schedule.

The format of the structured text files used to exchange data between the receiving Web site and the New York State Department of Environmental Conservation is shown in Appendix A.

46.2 How Pilot Participants Access the Web Site

In the DMR pilot, the pilot participants will identify themselves to the receiving Web site by entering a logon ID and password which is provided to the pilot participants by the New York State Department of Environmental Conservation. This logon ID and password is linked to the submitter’s facility and determines which permit number will be used to select the subset of DMRs which will be available to a given pilot participant for creation, editing, submitting and viewing. The login ID and password also determines which set of facility data will be used to pre-populate the DMR when the pilot participant selects a particular monitoring period and discharge number. [The login ID and password controls access to the receiving Web site, but has no relationship to the digital signature used by the submitter to sign the DMR. Facilities are permitted to create additional login IDs and passwords which give access to the DMRs under the control of the facility without any additional interaction with the New York State Department of Environmental Conservation.]

46.3 Phases of Tests

The DMR pilot will be organized in two phases. In the first phase, pilot participants will apply a cryptographic digital signature to the completed DMR before submitting the DMR to the receiving Web site. In order to be able to use the cryptographic digital signature mechanism, the pilot participants will need to perform a one-time setup procedure which includes the following steps:

- install a smart card reader on their computers,
- provide identity information to the certificate authority
- generate a public-private cryptographic key pair using their smart card,
- register a certificate with the certificate authority.

In the second phase of the DMR pilot, pilot participants will apply a biometric handwritten digital signature to the completed DMR before submitting the DMR to the receiving Web site. In order to be able to use the biometric digital signature mechanism, the pilot participants will need to perform a one-time setup procedure which includes the following steps:

- install a graphics tablet on their computers,
- enroll five handwritten signature samples using a pen provided with the graphics tablet.

Each phase of the pilot will last approximately two months, during which the pilot participants will be asked to resubmit electronic DMRs containing the same data which the pilot participants had previously submitted to the New York State Department of Environmental Conservation as official submissions in paper format over a previous six-month period. The New York State Department of Environmental Conservation will then compare the electronic DMR data received in the pilot with the data which had been previously received in paper format.

52.1 Description of Test Environment

The DMR pilot test environment consists of customized configuration of off-the-shelf hardware and software components which the pilot participants will install on their computers. These components will enable the pilot participants to load, display, edit sign, and submit DMR forms in an interactive manner while the participants are connected to a receiving Web site established for this purpose. A complete public key infrastructure (PKI) will be established for the pilot. Pilot participants will interact with the certificate authority supporting the DMR pilot’s PKI to establish certificates which will be used to authenticate the cryptographic digital signatures which they will apply to the DMR forms they submit.

Pilot participants will interact with standard HyperText Markup Language (HTML) forms to select DMR forms and navigate within the receiving Web site, but a special electronic forms environment (Adobe Acrobat Exchange Version 3.01) implemented as a plug-in to the participant's Web browser, will be used to display, edit, and submit the DMR forms. Using a digital signature plug-in to the electronic forms environment, pilot participants will apply digital signatures (cryptographic in Phase 1 and biometric in Phase 2) to each component of the overall DMR submission for any given permit number and monitoring period end date identified by a single discharge number or comment. The receiving Web site will authenticate the digital signatures, store the submitted data in a database and send the data to the New York State Department of Environmental Conservation for verification.

52.1.1 Installation and Setup

Pilot participants will be given an installation guide customized for the DMR pilot which lists the steps required to install the software components needed for the DMR pilot. Part of this installation will involve an upgrade to a consistent Web browser version to be used in the pilot. To assist the pilot participants in keeping in sync with the guide as they install the software components, snapshots of key screens will be included to assist the pilot participants in matching what they see on their computer monitor with the flow of steps in the installation guide. Staff from the New York State Department of Environmental Conservation (and in some cases also from Information Dynamics, Inc.) will be present at the participant's facility to assist with the installations as required, but the pilot participant will be encouraged to perform as much of the installation as possible based on the installation guide. Pilot participants will perform the required hardware installations (of the smart card reader in Phase 1 and the graphics tablet in Phase 2) to the degree they are able based on the standard installation instructions which ship with these products.

52.1.2 Using the Certificate Authority

In Phase 1, pilot participants will follow instructions contained in the customized installation guide to complete the enrollment and certificate registration steps needed to set up each pilot participant to subsequently apply a digital signature to DMR forms. Participants will accomplish the enrollment step by accessing a Web site maintained by the certificate authority for the pilot. Participants will then use their Web browser to supply identity information (e.g., name, company, facility, E-mail address) by filling out a HyperText Markup Language (HTML) form and submitting these identity data to the certificate authority. The New York State Department of Environmental Conservation, acting as the Local Registration Authority within the public key infrastructure established for the pilot, will be given secure access to these data from a Web browser and will approve, approve with modification, or reject the identity information provided by the pilot participants.

If the pilot participant's identity information is approved by the New York State Department of Environmental Conservation, the pilot participant will receive via E-mail a one-time access code which will allow the pilot participant to generate a public-private cryptographic key pair using the participant's smart card (supplied with the smart card reader), and register, using software provided by the certificate authority, an X.509 certificate with the certificate authority consisting of the participant's public cryptographic key and the participant's approved identity information.

If the pilot participant's identity information is modified or rejected by the New York State Department of Environmental Conservation, then the pilot participant will be automatically notified of this decision by E-mail. If the New York State Department of Environmental Conservation suggests modifications to the pilot participant's identity information, the body of the E-mail message sent to the pilot participant will contain a reference to a dynamically created Web page which will show what modifications are being suggested and request that the pilot participant approve or reject the modifications.

52.1.3 Using the Receiving Web Site

Pilot participants will be supplied with a customized user guide to help in the use of the Web site established for the DMR pilot. Participants will use a Web browser on their computer to access the Web site established to publish DMRs which are pre-populated with data appropriate to a given facility, permit number and monitoring period. Pilot participants will also submit their signed DMR data to this site, which for the purposes of the pilot will be called, the "receiving Web site".

Access to the receiving Web site is controlled by a login ID and password combination which is provided to the participant by the New York State Department of Environmental Conservation. The participant enters this login ID and password in the initial login Web page for the receiving Web site. The login ID and password combination determines what permit number should be used to select which DMRs can be accessed. The participant is given the option to use an administrative Web page to establish additional login IDs and passwords. These additional login IDs inherit the same access rights as the original, and enable a facility to grant access to the DMRs related to the facility's permit to other personnel within the participant's company or organization.

After successfully logging in to the receiving Web site, pilot participants can select a monitoring period and a DMR component (either a discharge number or comment) from a database-driven menu structure on a Web page. Pilot participants can then select whether they wish to start with a new form associated with this component, load a particular internal version of a form which has been accessed before but not submitted, or review forms which have already been submitted to the New York State Department of Environmental Conservation (external versions).

52.1.4 Design Considerations for the Electronic Form Environment

The DMR pilot will use a special electronic form environment when displaying, editing, signing and submitting DMR forms. This design decision was motivated by the need to:

- create a workable transition from paper to electronic formats. [The New York State Department of Environmental Conservation expressed the need to allow the DMR submitter, in a possible future production environment, to print copies of the DMRs they have submitted electronically, sign these paper DMR copies with ink, and keep the signed paper copies for review at the time of a site audit. The retention of paper copies of the DMR at the submitter's facility was seen as a more practical alternative to the long-term retention of electronic documents for most submitters.]
- provide an intuitive human interface to the electronic form which is not a significant conceptual change from the organization of a paper form. [A previous pilot test involving pilot participants interacting with standard HTML form versions of the Sub-monitoring Report (SMR), showed that these pilot participants experienced difficulty with the concept of scrolling within their Web browsers if the SMR was displayed as a single form, but the pilot participants also experienced difficulty in moving among multiple Web pages to fill out subforms which did not require horizontal scrolling. Also, the standard HTML forms did not display in the same way across the different browsers and computer platforms used by the pilot participants.]
- be able to claim that the electronic representation of the DMR form which is digitally signed produces a consistent visual display for all signers across multiple computer platforms (e.g., browsers, operating systems, monitors, etc.). [This may be necessary to support the argument that an electronic digital signature applied to the electronic representation of a document is meaningful because this electronic representation bears a consistent and faithful relationship to the visual display the signer is seeing when the signature is executed.]
- allow a digital signature to be applied to the entire contents (template plus data) of the form at the time the signer sees the visual representation of the form and executes the signature. [A digital signature applied only to data

outside the context of the document to which the signer is given assent may not be meaningful.]

- interact with a Web site in such a way that DMR forms can be presented to the submitter already pre-populated with data appropriate to the submitter's facility, permit number, discharge number and monitoring period end-date. [The ability for the submitter to receive DMRs which are pre-populated with default information was judged to provide a level of burden reduction required to add value to using the electronic forms environment versus paper, as well as to improve data integrity.]

For the purposes of the DMR pilot, Adobe Acrobat Exchange Version 3.01, operating as a plug-in to the participant's Web browser, was selected to meet the above design requirements. Given this selection, another design decision was required to determine how much of the total DMR submission to present to the submitter at any one time, and a further decision was required to determine how much content of the submission would be signed with a single digital signature.

The volume of the total DMR submission content to be loaded into the electronic form environment at one time was limited to the component level (e.g., discharge number and comment) for the following reasons:

- There are technical (primarily computer memory) limitations to the volume of information which can be loaded in the electronic form environment at one time.

- Tracking separate versions of each DMR component was seen as an advantage, since it is possible that: 1) it is likely that modifications made to the DMR submission would affect only one component and, 2) in a possible future production environment, different individuals may enter data for different DMR components in preparation for subsequent signing and submission.

- Storing separate components of the DMR as they are prepared reduces the risk of loss of the entire DMR submission in the case of a computer failure.

- The discharge number and comment are logical conceptual ways to subdivide the entire DMR submission into components which can be more easily manipulated in an electronic environment.

Since one of the design goals of the DMR test environment was to create a digital signature process in which what the signer sees on the computer screen at the time of signing can be shown to correspond to the electronic representation of this visual image in the memory of the computer, a design decision was required related to the extent of "signature dilution" which would be tolerated in the pilot design. Signature dilution can occur when it becomes less and less likely that the scope of the content which the signer is signing can be viewed by the signer at the time the signature is executed. For the purposes of the pilot, a design decision was made that a single digital signature could apply to the whole of the content in the DMR component (e.g., discharge number or comment), no matter how many actual screen pages were necessary to display this content.

Whereas the signature dilution concern is related to the legal question, “What did I sign?”, there is a potential corresponding concern, “Why did I sign?”. A rebuttable argument could be made that just because a signer performs some technical procedure to execute a digital signature, this does not necessarily record what intent the signer is conveying by these acts. In Phase 2 of the DMR pilot, in conjunction with the use of biometric handwritten signatures, the signer will receive a “gravity prompt” which requests the signer to indicate the purpose and intent of the digital signature before completing the signing process.

A sample of the design discussion related to signature dilution and gravity prompts is reproduced in Appendix B.

61.0.1 Using the Electronic Form

After the pilot participant selects a monitoring period and a form corresponding to the desired DMR component (e.g., discharge number or comment) using a Web browser connected to the pilot’s receiving Web site, the electronic form application installed on the participant’s computer will automatically launch and display the DMR form. If the selected component is the DMR information associated with a particular discharge number, the displayed electronic form will be pre-populated with data appropriate to the permit number, monitoring period and discharge number (including parameters to be monitored and their limit values). If the selected component is a comment, then the comment will be pre-populated with data appropriate to the permit number and monitoring period. The electronic form will also be pre-populated with visible internal and external version numbers so that a printed copy of the electronic form can be linked to the electronic submission.

Pilot participants can add data in data entry fields on the electronic form using the cursor or tab key to select the field and then typing in the desired data. Zoom and scrolling features are provided by the electronic form environment. After making all the data entry desired for the session, the participant can then either “prepare”, “save” or “submit” the form by selecting a menu button located at the bottom of the form. If the “prepare” option is selected, the data entered by the participant are sent across the Internet to the receiving Web site and stored in the database. An additional selection will appear on the Web page used to select DMR forms indicating that a new internal version of this particular DMR component exists. If the “save” option is selected, the data entered by the participant are sent to the receiving Web site as before, put the selection page will indicate that the new internal version has been “completed”.

The “submit” option indicates that the pilot participant is ready to submit the DMR component to the New York State Department of Environmental Conservation as an official submission. The pilot participant must apply a digital signature before the “submit” option is selected, or the receiving Web site will reject the submission.

61.0.2 Applying the Digital Signature

To apply a digital signature to a DMR form component, the submitter will click on an icon found inside the signature block on the last page of the electronic form. This will activate a digital signature plug-in which will prompt the signer to perform the selections and actions required to complete the signature.

When using a cryptographic signature in Phase 1 of the pilot, the signer will be prompted to select a certificate, signing algorithm, and cryptographic service provider. Then the signer will be prompted to enter a four-digit personal identification number (PIN) which has been previously established as an access control mechanism for the signer’s smart card. After the smart card has supplied the private key to the digital signature plug-in, and the digital signature plug-in has calculated the digital signature hash based on this private key and the content of the form, the digital signature plug-in window will close and a check mark will appear on the signing icon in the signature block of the form.

When using the biometric handwritten digital signature in Phase 2 of the pilot, the signer will be prompted to enter the signer’s name and reason for signing. The signer will then be given the option to begin the capture of the biometric handwritten signature. When the signer begins the capture process, the signer will execute a handwritten signature using a special pen and graphics tablet. The signer has the option of either repeating the handwritten signature or indicating that the signature is complete. When the signature is complete, and the digital signature plug-in has received the signature dynamics data from the graphics tablet (e.g., acceleration, wobble, timing, etc.), and has bound these data to the form content using a cryptographic algorithm, the digital signature plug-in window closes and a vector graphic representation of the handwritten signature appears in the signature block on the form.

61.0.3 Submitting the DMR Data

After the DMR form has been signed, the submitter will press the “submit” button located at the bottom of the form. This will send the data entered by the participant, along with the digital signature, across the Internet to the receiving

Web site. The receiving Web site will reconstruct the DMR form content as it existed on the submitter's computer at the time the digital signature was applied. This reconstructed content will be used to validate the digital signature received at the Web site, along with the public key found within the certificate of the signer (if the digital signature is cryptographic) or an automated pattern recognition of signature dynamics data which has been trained by the previous receipt of enrollment signatures (if the digital signature is biometric).

If the receiving Web site validates the digital signature, the data submission will be accepted and stored in the receiving Web site's database. If the digital signature cannot be validated, the receiving Web site will reject the submission and notify the signer by means of a Web page.

Once the submitted data have been accepted by the receiving Web site, the receiving Web site will attempt a preliminary validation of the data and create an automatically-generated Web page notifying the submitter of potential errors. The submitter then has the option of directing the receiving Web site to accept the submission "as is" with no further correction, or to redisplay the form with its submitted data for the purpose of further editing and a subsequent resubmission.

Once the form data have been successfully submitted, the DMR form with the submitted data can be viewed at the receiving Web site by anyone who logs on to the Web site with a login ID and password which has access rights to the DMR form data.

61.1 Design of Public Key Infrastructure for Pilot

A complete public key infrastructure (PKI) will be established to support Phase 1 of the DMR pilot. A certificate authority (CA) and a local registration authority (LRA) will be established and operated for use by the pilot participants and the New York State Department of Environmental Conservation (NYS DEC). The following diagrams show the interaction of the CA and LRA with the pilot participants. For the purposes of the pilot, a third-party (E-Lock Technologies, Inc.) will act as the CA and the NYS DEC will act as the Local Registration Authority.

A suggested Statement of Service provided by the CA for the DMR pilot is reproduced in Appendix C.

Preparing for Electronic Reporting–Finalizing the Agreement

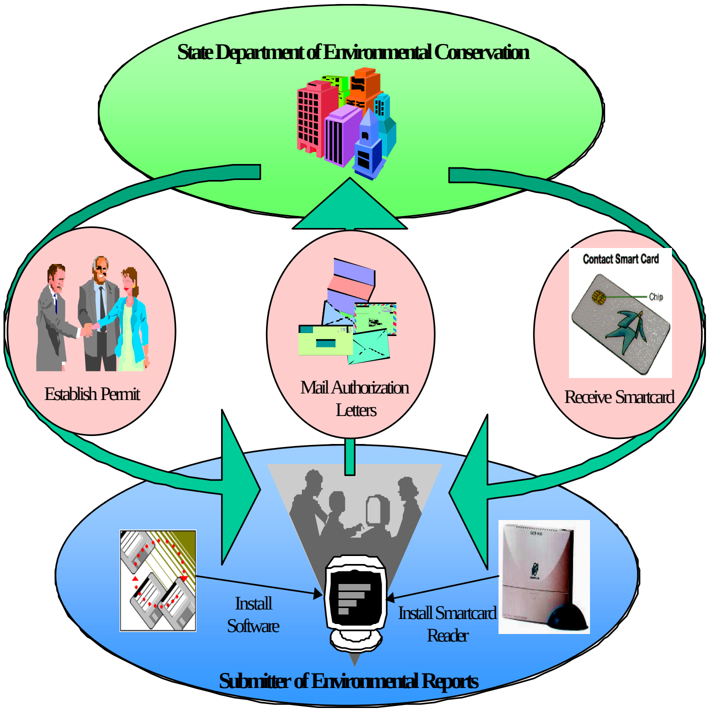
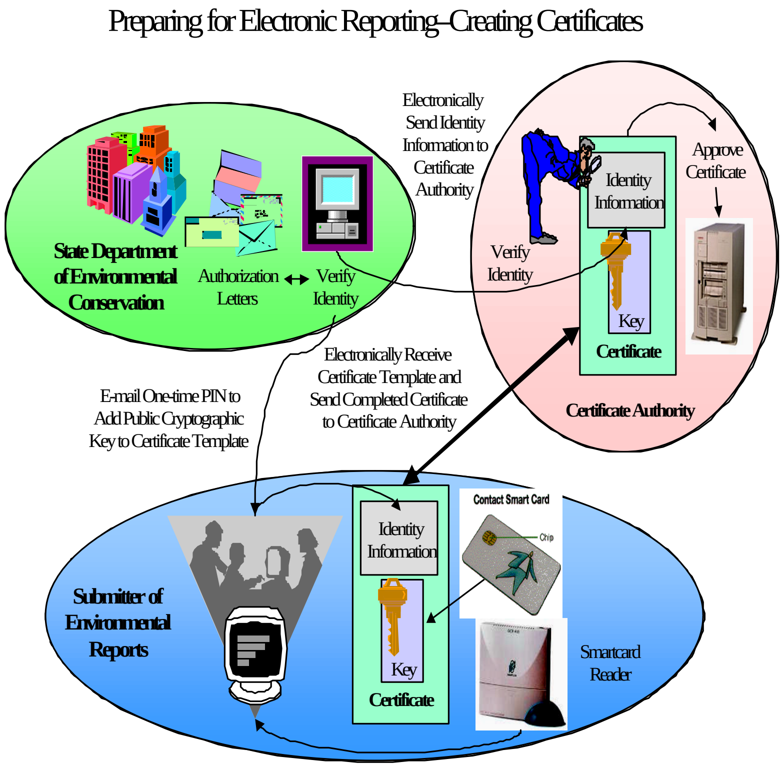

State Department of Environmental Conservation
Establish Permit
Mail Authorization Letters
Contact Smart Card
Chip
Receive Smartcard
Install Software
Install Smartcard Reader
Submitter of Environmental Reports

Figure 1

As shown in Figure 1, the design of the PKI for the DMR pilot assumes that NYS DEC has prior knowledge of the submitters through paper documents and other forms of contact. It is also assumed that NYS DEC has verified these identity data and has established an agreement (a “permit”) with each submitting company. The permit specifies the reporting requirements. NYS DEC provides a smartcard to each submitter who will be electronically signing Discharge Monitoring Reports (DMRs). The submitter installs a smart card reader and software which allow the submitter to use the smart card.

As shown in Figure 2, NYS DEC also acts as a Local Registration Authority (LRA) by approving the identity information for each submitter. After NYS DEC has approved the identity information, NYS DEC releases an E-mail message to be sent to the submitter. The E-mail message (automatically generated by the CA but triggered by NYS DEC’s approval using an LRA administrative console provided by the CA) contains a one-time access code or personal identification number (PIN). While connected over the Internet to the Certificate Authority, the submitter inserts the smart card into the smart card reader attached to the submitter’s computer, enters a four-digit code which activates the smart card, and then uses the smart card to generate a cryptographic key pair. The submitter uses the PIN number received from NYS DEC and software provided by the CA to join the submitter's public cryptographic key to the identity information previously approved by NYS DEC.

Figure 2


Preparing for Electronic Reporting–Creating Certificates
State Department of Environmental Conservation
Authorization Letters
Verify Identity
Electronically Send Identity Information to Certificate Authority
Identity Information
Approve Certificate
Verify Identity
Key
Certificate
Certificate Authority
E-mail One-time PIN to Add Public Cryptographic Key to Certificate Template
Electronically Receive Certificate Template and Send Completed Certificate to Certificate Authority
Contact Smart Card
Chip
Identity Information
Key
Certificate
Submitter of Environmental Reports
Smartcard Reader

As a result of this procedure, the submitter's smartcard is programmed to generate the submitter's private cryptographic key, and the Certificate Authority receives a completed X.509 certificate with the submitter's identity information and the submitter's public cryptographic key. A duplicate copy of the submitter's certificate is also stored on the submitter' computer.

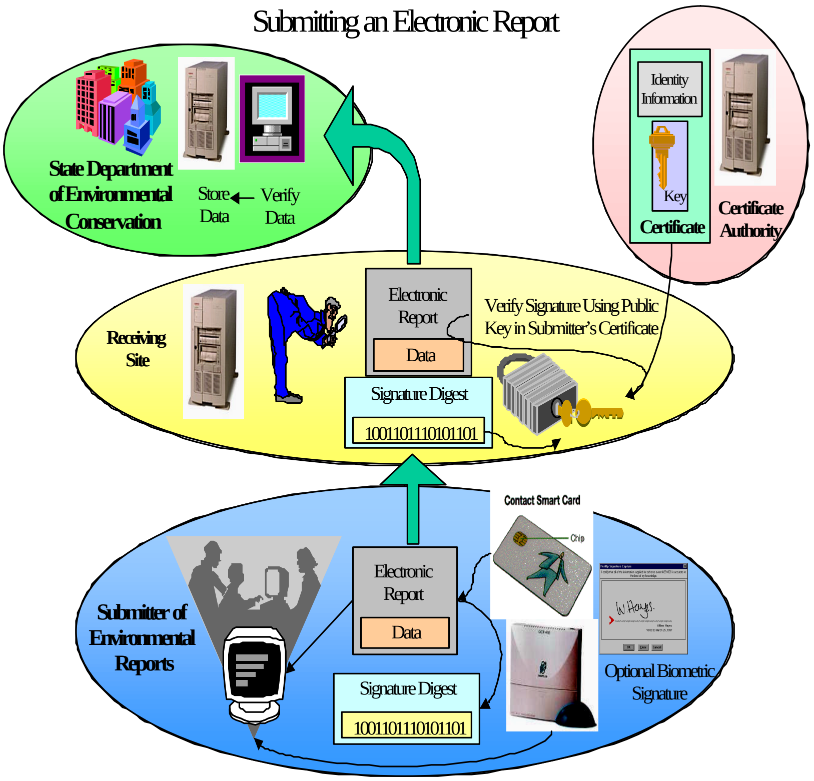


Figure 3

As shown in Figure 3, after the above setup procedures are completed the submitter subsequently fills out Discharge Monitoring Reports by using a browser to log in to a receiving Web site established for the pilot. Based on the identity of the submitter, the receiving Web site automatically prepares a form template pre-loaded with identity and reporting requirement information appropriate to the submitter. This pre-loaded form template automatically downloads to the submitter's computer. The submitter then completes the form with the necessary values for the required reporting fields. When the form is ready to submit, the submitter inserts the submitter's smart card in the smart card reader and enters a four digit code to activate the smart card. As a result of this action, cryptographic software installed on the submitter's computer calculates a digital signature based on the submitter's private cryptographic key and the entire contents of the completed form. [In some configurations, the submitter signs their handwritten signature on an attached graphics tablet using an electronic pen.] The submitter then presses a submit button to send the completed form data over the Internet to the receiving Web site.

When the completed data are received at the Web site, the data are stored in the Web site's database. To verify the submitter's signature, the data stored in the database are combined with the form template originally prepared for the submitter to create a reconstructed form at the Web site. The Web site uses the submitter's public cryptographic key contained within the submitter's certificate to verify that the submitter signed the completed form and that the completed form as reconstructed at the Web site is identical to the completed form as it existed on the submitter's computer at the time it was signed. If a biometric handwritten signature was used, the biometric signature is verified using a pattern recognition application previously trained with a set of enrolled handwritten signatures.

After the submitter's signatures are verified at the receiving Web site, a complete set of form data are transferred as an electronic file over the Internet to NYS DEC. NYS DEC then checks for completeness and data errors.

Appendix A

62 Information to be Pre-populated on the DMRs

DMRs on the Web Facility Information

	Acronym	**Description**	**Length**
9	NPID	SPDES Number	9
15	MVDT	Monitoring Period End Date	6
1	ANAM	Alternate Mailing Name	30
2	AST1	Alternate Street Address #1	30
3	AST2	Alternate Street Address #2	30
4	ACTY	Alternate City	23
5	ASTT	Alternate State	2
6	AZIP	Alternate Zip Code	9
7	NAM1	Facility Name -Part 1	30
8	OFFL	Cognizant Official	30

DMR's on the Web Comments Information

9	NPID	SPDES Number	9
15	MVDT	Monitoring Period End Date	6
10	PLDS	Discharge Number	3
11	PLRD	Report Designator	1
12	PIPE	Pipe Description	30
13	SUBR	DEC Region	2
34	PIC1	DMR Comments Field -Part 1	35
35	PIC2	DMR Comments Field -Part 2	35
36	PIC3	DMR Comments Field -Part 3	35
37	PIC4	DMR Comments Field -Part 4	35
38	PIC5	DMR Comments Field -Part 5	35
39	PIC6	DMR Comments Field -Part 6	35
40	PIC7	DMR Comments Field -Part 7	35
41	PIC8	DMR Comments Field -Part 8	35
42	PIC9	DMR Comments Field -Part 9	35

The DMR form should have the certification box printed on the bottom of the DMR.

DMR's on the Web Limits Information

9	NPID	SPDES Number	9
14	*	Monitoring Period Start Data	6
15	MVDT	Monitoring Period End Date	6
10	PLDS	Discharge Number	3
11	PLRD	Report Designator	1
16	PRAM	Parameter Code	5
16b	PRAS	Parameter Code Description	29
17	MLOC	Monitoring Location	1
17b	MLOCD	Monitoring Location Description	20
18	SEAN	Seasonal Indicator	1
19	MODN	Modification Number	1
20	LQAV	Limit Quantity Average	8
21	LQASS	Quantity Ave. Statistical Base Desc.	8
22	LQMX	Limit Quantity Maximum	8
23	LQXSS	Quantity Max. Statistical Base Desc.	8
24	LQUCD	Limit Quantity Units Description	12
25	LCMN	Limit Concentration Minimum	8
26	LCMS	Conc. Min. Statistical Base Desc.	8
27	LCAV	Limit Concentration Average	8
28	LCASS	Conc. Ave. Statistical Base Desc.	8
29	LCMX	Limit Concentration Maximum	8
30	LCXSS	Conc. Max. Statistical Base Desc.	8
31	LCUCD	Limit Concentration Units Description	12
32	FRAND	Frequency of Analysis Description	15
33	SAMPD	Sample Type Description	6

DMR's on the Web Measurement Information

9	NPID	SPDES Number	9
14	*	Monitoring Period Start Date	6
15	MVDT	Monitoring Period End Date	6
10	PLDS	Discharge Number	3
11	PLRD	Report Designator	1
16	PRAM	Parameter Code	5

17	MLOC	Monitoring Location	1
18	SEAN	Seasonal Number	1
19	MODN	Modification Number	1
43	MQAV	Measurement Quantity Average	8
44	MQMX	Measurement Quantity Maximum	8
45	MCMN	Measurement Concentration Minimum	8
46	MCAV	Measurement Concentration Average	8
47	MCMX	Measurement Concentration Maximum	8
48	REXC	Reported Number of Excursions	2
49	RFRQ	Reported Frequency of Analysis	5
50	RSAM	Reported Sample Type	2
	NODI	No Discharge codes for each DMR measurement line.	

DMR’s on the Web Memo Information

9	NPID	SPDES Number	9
14			

*MonitoringPeriodStartDate6

1

5MVDTMonitoringPeriodEndDate6

1

0PLDSDischargeNum

ber3

1

1PLRDReportDesignator1

Memo Field ?

Appendix B

63 Signature Dilution when Signing Long Forms

-----Original Message-----
From: Ben Wright [mailto:Ben_Wright@compuserve.com]
Sent: Thursday, January 14, 1999 2:06 PM
To: Todd Lewis
Cc: Jeffrey Sandler
Subject: signing long EPA forms

Todd said:
>>If the digital signature is applied once at the bottom of the form, does the fact that the signer cannot conveniently see the entire contents in one screen context dilute the meaning of the digital signature?<<

I do believe there is a "dilution" problem. The issue is that for EPA a signature should be a meaningful event that informs the signer about what is being signed and that displays his deliberation over the signed material. This event should be recorded.

In the paper world, we sometimes deal with this problem by having the signer initial pages or initial selected clauses. (When I rent a car, the rental company asks me to sign and initial the one-page contract in 4 different places!)

There might be any number of solutions to this in the electronic world. The objective is to force the signer through some human-meaningful ritual that makes clear he is becoming responsible for the whole form. This seems especially important for EPA because EPA wants to motivate the signer to check the form, check the facts and take direct personal action to ensure compliance. EPA wants the signer who signs an inaccurate form to lose sleep at night because he knows what the form said and knows there was an inaccuracy. The signature should help to engage his conscience.

One idea, using PenOp as it is designed today: Have the signer sign with PenOp in multiple places. A signature need not necessarily be at the bottom of every screen or every page. Instead, the signature might be gathered at 3 or 4 strategic places in the document. The "gravity prompt" for the first 2 or 3 signatures might be different from the gravity prompt in the last signature. (Gravity Prompt is PenOp's term the reason-for-signing sentence that appears at the top of a signature box while the signer writes his autograph.) The first 2 or 3 gravity prompts might say something like "I sign this document here to show that I am personally responsible for the whole document and each item in it." Then, the gravity prompt for the final signature might be a more legal statement like "This is my legal signature to the form."

>>If so, does the concept of requiring the signer to acknowledge each row of the form with a radio button add any value to the digital signature which is ultimately applied?<<

This idea could help. However, I'm not sure how you keep a convenient record that each radio button was clicked, or that they were clicked by the signer and not his assistant. In theory a system could be created to record when the radio buttons were clicked and so on, but that is probably a lot more software development work than just requiring the signer to sign 3 or 4 times as I suggested above.

Does this help? I'd be happy to discuss further.

--Ben

-------------Forwarded Message-----------------

From: "Lewis, Todd", INTERNET:TLewis@idinc.com
To: "'Ben Wright'", Ben_Wright

Date: 1/13/99 8:31 PM

Ben, do you have any comment on the legal significance of Point 3 in the E-mail message below? This suggestion tries to solve the problem of a long electronic form which requires a digital signature. The form is sufficiently long that the signer would need to scroll extensively to view it before applying the digital signature. If the digital signature is applied once at the bottom of the form, does the fact that the signer cannot conveniently see the entire contents in one screen context dilute the meaning of the digital signature? If so, does the concept of requiring the signer to acknowledge each row of the form with a radio button add any value to the digital signature which is ultimately applied?

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Chuck Haugh [mailto:cshaugh@gw.dec.state.ny.us]
Sent: Tuesday, January 12, 1999 9:29 AM
To: nelson.kimberly@epamail.epa.gov; tlewis@idinc.com
Cc: vann.roger@epamail.epa.gov; mustreet@gw.dec.state.ny.us; sevogler@gw.dec.state.ny.us
Subject: Items for Thurs. conf. call

Steve, Meredith and I have been thinking about other items we have to consider for the pilot, and have come up with the following.

1. Comments submitted by the permittee - about 35% of DMRs submitted via paper have an attachment with them, or comments written on the bottom of the DMR page. Our prepopulated file contains fields for comments on the bottom of the preprinted DMR form (items 34 - 42). We suggest a comments button on the bottom of the form that allows the permittee the capability of opening a memo type field that they can fill out and submit with the DMR. We should limit the size to a reasonable length.

2. Many facilities will have a lab person fill out the DMR, and forward it to a supervisor to review and sign. Can we build into the pilot the capability of a lab person filling in the info. and then saving the filled in form and having the supervisor review, sign, and send the Web DMR in? i.e. multiple web sessions.

3. Steve had an alternative to having them signing each Page of Web DMR. In our EDV system that allows us to review electronic submissions on a parameter by parameter basis, we use a radio button on each line to accept reported values.

He was wondering if we could build in the same functionality for the Web DMRs; i.e., have the permittees have to accept reported values on a line by line basis, and use that as the method of making the permittees acknowledge that the values they are submitting they have reviewed prior to the submission in addition to the certification of the whole DMR.

Steve is reworking the prepopulated file to include description fields, and we hope to send it out later today. We have had 4 facilities volunteer so far, and I hope to have the other two by the end of the week. We have had two people from EPA region 2 ask to kept informed of the pilot project, they are both on the Computer side of things. I will send an E-mail to the program people and let them know what is happening also.

Appendix C

64 EPA Pilot CA Project Statement of Service

Draft

10th March 1999

64.1 Introduction

This document briefly discusses the certification services offered by the E-Lock CA, as part of the EPA Pilot CA Project, and the practices adopted in effecting those services. Note that this document is not a complete Certification Practices Statement (CPS) but rather a proposal for the services and practices adopted by the E-Lock CA for its certification services to be offered to EPA.
It also discusses various other relevant technical issues and procedures to be adopted by the participating entities as part of the project.

64.2 Practice Statements, Rights and Obligations

This section lists the practices adopted by E-Lock CA, rights and obligations on part of all participating entities viz. the E-Lock CA, issuing or local registration authority (LRA), the end user or subscriber and any relying parties in the provision of E-Lock's certification services (CS). The certification practices are employed in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI). It details and controls the certification process, from establishing LRAs, commencing LRA and repository operations, to enrolling subscribers. The certification services provide for issuing, managing, using, revoking, and renewing of certificates. The CPS is intended to legally bind and provide notice to all parties that create, use, and validate certificates within the context of the CS. As such, the CPS plays a central role in governing the CS.

1. In absence of a complete Certification Practice Statement (*see* definitions), the relevant sections in this document, including these statements, control the provision and use of E-Lock's public certification services (*see* definitions) – including certificate (*see* definitions) application, application validation, certificate issuance, acceptance, use, and revocation.

2. You (the user) acknowledge that (i) you have been advised to receive proper training in the use of public key techniques prior to applying for a certificate and that (ii) documentation, training, and education about digital signatures, certificates, PKI are available from E-Lock Technologies.

3. E-Lock offers different classes of certificates. You and the local registration authority must decide which class(es) of certificate are right for your needs.

4. Before submitting a certificate application, you must generate a key pair and keep the private key secure from compromise (*see* definitions) in a trustworthy (*see* definitions) manner. Your software system, in this case the E-Lock PKI Client application, should provide this functionality.

5. You must accept (*see* definitions) a certificate before communicating it to others, or otherwise inducing their use of it. By accepting a certificate (*see* definitions), you make certain important representations.

6. If you are the recipient of a digital signature or certificate, you are responsible for deciding whether to rely on it. Before doing so, E-Lock recommends that you check the E-Lock repository (*see* definitions) to confirm (*see* definitions) that the certificate (*see* definitions) is valid (*see* definitions) and not revoked (*see* definitions), and then use the certificate to verify that the digital signature (*see* definitions) was created during the operational period of the certificate by the private key (*see* definitions) corresponding to the public key (*see* definitions) listed in the certificate (*see* definitions), and that the message (*see* definitions) associated with the digital signature (*see* definitions) has not been altered.

7. You agree to notify the applicable issuing authority (*see* definitions) upon compromise (*see* definitions) of your private key (*see* definitions).

8. The LRA designated by E-Lock CA would be solely responsible for validating or proofing the certification requests and any relevant information supplied by the end user for getting a certificate.

9. This document would be publicly available at the following secure site https://www.epa-ca.com/CS

10. This document (*see* definitions) provides various warranties made by E-Lock and the issuing or local registration authorities. Otherwise, warranties are disclaimed and liability is limited by E-Lock CA and issuing authorities.

64.3 Services Proposal

E-Lock Technologies would own, operate and maintain a dedicated Certification Authority (CA) as part of the EPA pilot project. Any access to the CA would strictly be restricted and limited only to trustworthy E-Lock Technologies administrative staff.
The CA would use RSA algorithms to generate its keys, and sign all certificates. All certificates issued would follow X509 v3 specification.

The E-Lock CA would assume the following name(subject DN):
cn=NY DMR Pilot E-Lock CA, ou=EPA Pilot, o=IDI/EPA, l=Albany, st=NY, c=US

The E-Lock CA would create a local registration authority (LRA) and would designate an administrator (LRAA) who would be responsible for registering, proofing EPA participants and managing the LRA. The LRA would be created to adopt the following naming for all participant or end-user certificates:
cn="Your choice", mail=enduser mailaddress, o=IDI/EPA, st=NY, c=US

The E-Lock CA would issue a certificate for the LRA administrator. The LRA Administrator would use a smart-card to generate his key-pair that would be associated with his certificate. The LRAA would use the smart-card to access the LRA administrator console.

To facilitate the end user registration process, a web form would be made available that would be used by the EPA participants or end users to enter their personal or identity information which would be used to issue a certificate. This information would be entered in a staging database for later validation and/or verification by the LRAA.

The LRAA would be responsible for doing the proofing and validation on the information in the staging database as per EPA requirements. He/she then would register the user with the LRA, enable him for certification by creating a certificate profile.
The information in the certificate profile would be used to construct the certificate for the user. Given our understanding of the certificate requirements for the pilot, signature keyusage certificate extension should be enabled in the profile. If desired, E-Lock can fabricate a custom profile for the purpose. On activation, the certificate profile would generate a PIN. This would amount to certificate request approval.

The PIN then would be sent to the user's email address as available in the user information. This mechanism would serve as a verification check on the end-user's email address.

The end user would then use the E-Lock PKI Client application, supply the PIN and submit a request to the E-Lock CA. On successful processing, the certificate would be installed on the end user system.

The E-Lock CA would publish all certificates and CRLs on E-Lock repository. The information, certificates and CRLs, in E-Lock repository would be accessible over LDAP v2.
The E-Lock CA would also make available a OCSP service accessible using the E-Lock PKI Client application that can be used to check the revocation status of any certificate issued by the E-Lock CA in an online fashion.

The EPA participants or end users should contact the designated LRAA for requests for additional certificates, certificate renewals and reporting any key compromises.

The E-Lock CA would backup the signing key-pair of the E-Lock CA in a secure manner. It would also backup all LRA, end user information along with all certificates issued in a secure manner from time to time. The E-Lock CA would also log all activities like certification requests, along with their outcomes.

64.4 Table of Acronyms and Abbreviations

CA	certification authority
CPS	Certification Practice Statement
CRL	certificate revocation list
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IA	issuing authority
LRA	local registration authority
LRAA	local registration authority administrator
CA	Certification authority
CS	certification services
PIN	personal identification number
PKCS	Public Key Cryptography Standards
PKI	public key infrastructure
RDN	Relative Distinguished Name

RSA	a cryptographic system (*see* definitions)
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
X.509	the ITU-T standard for certificates and their corresponding authentication framework